REMARKS

Applicants wish to thank the Examiner for the attention accorded to the instant application, and respectfully request reconsideration of the application as amended.

Formal Matters

Claims 1-10 were pending in the Application. By this amendment, claims 2-5 are amended and claims 1 and 6-10 are canceled without prejudice. Specifically, claims 2-5 are amended to more clearly recite the invention and to correct minor errors. For example, claims 2 and 3 are amended to recite stopping when the sequential substitution reencryption process has been performed for all calculation devices; support for this amendment can be found in the original specification at least on page 30, lines 11-13 and in Figure 9. Claims 2 and 3 are also amended to recite an ElGamal cipher text preparation step in which at least one of the computers generates a set of ElGamal cipher texts corresponding to inputs of the gates of the circuit that realizes the given function; support for this amendment can be found in the original specification at least on page 28, line 9 through page 29, line 12.

Upon entry of this amendment, claims 2-5 are pending in the application, with claims 2 and 3 being independent claims. Care has been taken to ensure no new matter is being entered.

Claim Objections

Claims 1-10 are objected to because of informalities. Claims 2-5 are amended to correct informalities and minor errors. Claims 1 and 6-10 are canceled. Withdrawal of these claim objections is respectfully requested.

Rejection of Claims Under 35 U.S.C. §112

Claims 1-10 are rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement because these claims do not include a stopping condition. Claims 2-

5 are amended to include a stopping condition of stopping when all the computers have performed the sequential substitution reencryption process. Claims 1 and 6-10 are canceled, rendering their rejection moot.

Claim 6 is rejected under 35 U.S.C. § 112, second paragraph. Claim 6 is canceled, rendering its rejection moot.

Withdrawal of these rejections is respectfully requested.

Rejection of Claims Under 35 U.S.C. §102

Claim 1 is rejected under 35 U.S.C. § 102(b) as anticipated by "The Round Complexity of Secure Protocols" by Beaver et al. (hereinafter "Beaver"). Claim 1 is canceled, rendering its rejection moot. Withdrawal of this rejection is respectfully requested.

Rejection of Claims Under 35 U.S.C. §103

Claims 2-4 are rejected under 35 U.S.C. § 103(a) as unpatentable over Beaver in view of Furukawa, U.S. Patent Application Publication No. 2002/0181702. Claim 5 is rejected under 35 U.S.C. § 103(a) as unpatentable over Beaver in view of Furukawa, and further in view of U.S. Patent No. 6,195,433 to Vanstone et al. (hereinafter "Vanstone"). Claims 6-9 are rejected under 35 U.S.C. § 103(a) as unpatentable over Beaver in view of Furukawa, and further in view of Vanstone. Claim 10 is rejected under 35 U.S.C. § 103(a) as unpatentable over Beaver in view of Furukawa, and further in view of Vanstone and further in view of U.S. Patent No. 6,792,533 to Jablon. These rejections should be withdrawn based on the comments and remarks herein.

Claim 2 as amended herein recites the ElGamal cipher text preparation process comprises an ElGamal cipher text preparation step in which at least one of the computers generates a set of ElGamal cipher texts corresponding to inputs of the gates of the circuit that realizes the given function.

Claim 3 as amended herein recites the ElGamal cipher text preparation means prepares ElGamal cipher texts for generating a set of ElGamal cipher texts corresponding to inputs of gates of the circuit that realizes the function.

Accordingly, as amended herein, claims 2 and 3 recite that a set of ElGamal cipher texts is generated corresponding to inputs of gates of the circuit.

Beaver teaches a network of processors having a read-only common input tape and does not teach or suggest inputs of gates or generating a set of ElGamal cipher texts corresponding to input of gates, as recited in the claims of the present invention. Furukawa discloses a certified shuffle-decrypting technique in which encrypted texts, public keys and secret keys are input (paragraph [0047]). This technique can realize further high-speed processing by greatly decreasing the number of modular exponentiations and an amount of calculation (paragraph [0020]). Furukawa does not teach or suggest circuits, gates or inputs of gates. Hence, the combination of Beaver and Furukawa does not teach or suggest generating a set of ElGamal cipher texts corresponding to inputs of gates of the circuit.

Vanstone does not overcome this deficiency and the Examiner does not state otherwise. Vanstone is cited for allegedly teaching the generation of public/private keys. Without acquiescing to the correctness of the Examiner's interpretation of Vanstone, applicants submit that Vanstone does not teach or suggest generating a set of ElGamal cipher texts corresponding to inputs of gates of the circuit.

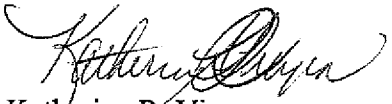
It has been held by the courts that to establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. See, *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). As illustrated above, the hypothetical combination of Beaver and Furukawa and Vanstone does not teach or suggest generating a set of ElGamal cipher texts corresponding to inputs of gates of the circuit, so that *prima facie* obviousness has

not been established. Thus, independent claims 2 and 3, along with their dependent claims, patentably distinguish over the art of record in the application. Claims 6-10 are canceled, rendering their rejections moot. Hence, withdrawal of this rejection is respectfully requested.

Conclusion

For the reasons set out above, Applicants respectfully submit that the application is in condition for allowance. Favorable reconsideration and prompt allowance of the application are respectfully requested. Should the Examiner believe that anything further is needed to place the application in even better condition for allowance, the Examiner is requested to contact the undersigned representative at the telephone number below.

Respectfully submitted,



Katherine R. Vieyra
Registration No: 47,155

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza, Suite 300
Garden City, New York 11530
516-742-4343

KRV:ch